Claims:

1. A message digest hardware accelerator for selectively processing multiple cryptographic hash algorithms, comprising:

a register file (12) having at least five registers for storing chaining variables;

a function circuit (22) receiving first (B), second (C) and third (D) chaining variables and an output that provides a logical data value;

a first multiplexer (24) having an input coupled to the register file for receiving a fourth (E) chaining variable and an output that provides the fourth chaining variable or a zero value; and

a summing circuit (30) having a first input coupled to the output of the function circuit for receiving the logical data value, a second input coupled to the output of the first multiplexer, and an output coupled to the register file.

2. The message digest hardware accelerator of claim 1, further comprising:

a barrel shifter (40) having an input coupled to the output of the summing circuit;

an adder (41) having an input coupled to an output of the barrel shifter; and

a second multiplexer (42) having a first input coupled to the output of the summing circuit and a second input coupled to an output of the adder.

3. The message digest hardware accelerator of claim 2, further comprising:

a third multiplexer (26) having a first input coupled to the output of the second multiplexer (42) and a second input coupled to the register file (12) for receiving a fifth (A) chaining variable; and

a fourth multiplexer (28) having a first input coupled to the output of the second multiplexer and a second input coupled to the register file (12) for receiving the third (D) chaining variable.

4. The message digest hardware accelerator of claim 3, wherein the second multiplexer and the fourth multiplexer receive a signal that transfers a summed value from the output of the summing circuit to the register file when the message digest hardware accelerator is processing an SHA-1 hash algorithm.

5. The message digest hardware accelerator of claim 3, wherein the second multiplexer and the third multiplexer receive a signal that transfers a summed value from the output of the barrel shifter to the register file when the message digest hardware accelerator is processing an MD5 hash algorithm.

6. The message digest hardware accelerator of claim 3, further comprising:

a first shift circuit (16) having an input coupled to the register file for receiving the first (B) chaining variable; and

a fifth multiplexer (14) having a first input coupled to an output of the first shift circuit, a second input coupled to the input of the first shift circuit and an output coupled to the register file for providing the second chaining variable.

7. The message digest hardware accelerator of claim 6, further comprising:

a second shift circuit (18) having an input coupled to the register file for receiving the fifth (A) chaining variable; and

a sixth multiplexer (20) having a first input coupled to an output of the second shift circuit, a second input coupled to the input of the second shift circuit and an output coupled to another input of the summing circuit.

8. A circuit for generating hash values in an SHA-1 mode and an MD5 mode, comprising:

a storage circuit (34, 36);

a register array (32) having registers for storing a message and an output for providing a round dependent data value (W_t);

a register file (12) for storing first (B), second (C), third (D), fourth (E) and fifth (A) chaining variables; and

a summing circuit (30) having a first input coupled for receiving a first set of constant values stored in the storage circuit for the SHA-1 mode and a second set of constant values for the MD5 mode, a second input coupled to the output of the register array, a third input coupled for receiving the fifth (A) chaining variable in the MD5 mode and a shifted fifth chaining variable in the SHA-1 mode, a fourth input coupled for receiving a logical function in accordance with the first, second and third chaining variables, and a fifth input coupled for receiving the fourth chaining variable in the MD5 mode and a zero value in the SHA-1 mode.

9. The circuit of claim 8, further comprising a first multiplexer (42) having a first input coupled to the register file (12) for receiving the fourth (E) chaining variable, a second input coupled for receiving zero value and an output coupled to the fifth input of the summing circuit.

10. The circuit of claim 9, further comprising:

a barrel shifter (40) having an input coupled to the output of the summing circuit;

an adder (41) having an input coupled to an output of the barrel shifter; and

a second multiplexer (42) having a first input coupled to the output of the summing circuit and a second input coupled to an output of the adder.

11. The circuit of claim 10, further comprising:

a third multiplexer (26) having a first input coupled to an output of the second multiplexer and a second input coupled to the register file for receiving the fifth (A) chaining variable; and

a fourth multiplexer (28) having a first input coupled to the output of the second multiplexer and a second input coupled to the register file for receiving the third (D) chaining variable.

12. The circuit of claim 11, further comprising:

a first shift circuit (16) having an input coupled to the register file for receiving the first (B) chaining variable; and

a fifth multiplexer (14) having a first input coupled to an output of the first shift circuit, a second input coupled to the input of the first shift circuit and an output coupled to the register file for supplying an updated second (C) chaining variable.

13. The circuit of claim 12, further comprising:

a second shift circuit (18) having an input coupled to the register file for receiving the fifth (A) chaining variable; and

a sixth multiplexer (20) having a first input coupled to an output of the second shift circuit, a second input coupled to the input of the second shift circuit and an output coupled to the third input of the summing circuit.

14. A message digest hardware accelerator integrated to provide a hash value of a variable length message in accordance with a first algorithm and a second algorithm, comprising:

a register file (12) having five registers preset to a first group of values for the first algorithm and to a second group of values for the second algorithm, the register file storing first (B), second (C), third (D), fourth (E) and fifth (A) chaining variables;

a function circuit (22) receiving first, second and third chaining variables and generating a first logical data value for the first algorithm and a second logical data value for the second algorithm;

a storage element (34, 36) for supplying a first set of constant values for the first algorithm and a second set of constant values for the second algorithm; and

a summing circuit (30) having a first input coupled to the output of the function circuit (22) and a second input coupled to the storage element for receiving one of the first and second sets of constant values.

15. The message digest hardware accelerator of claim 14, further including a register array (32) having a decoder circuit (120) for selecting a data word stored in one of the sixteen registers and supplying the data word to an output of the register array when computing the first algorithm.

16. The message digest hardware accelerator of claim 15, wherein the register array further includes:

sixteen registers that form a word wise circular queue;

an exclusive-OR (116) coupled for receiving first, second, third and fourth data words stored in the sixteen registers; and

a rotate block (118) having an input coupled to an output of the exclusive-OR and supplying a one bit left circular shift of the data generated by the exclusive-OR to one of the registers in the sixteen registers.

17. The message digest hardware accelerator of claim 14, wherein an output of the register array is supplied from the word wise circular queue when computing the second algorithm.

18. The message digest hardware accelerator of claim 14, wherein the first

algorithm is an MD5 algorithm and the second algorithm is an SHA-1 algorithm.